Hindawi
Security and Communication Networks
Volume 2021, Article ID 2949513, 10 pages
https://doi.org/10.1155/2021/2949513

Research Article

A Commitment Scheme with Output Locality-3 Fit for the IoT Device

Hideaki Miyaji,[1] **Yuntao Wang**,[2] **Akinori Kawachi**,[3] **and Atsuko Miyaji**[1,2]

[1]*Graduate School of Engineering, Osaka University, Osaka, Japan*
[2]*School of Information Science, JAIST, Nomi Shi, Japan*
[3]*Graduate School of Engineering, Mie University, Tsu, Japan*

Correspondence should be addressed to Hideaki Miyaji; hideaki@cy2sec.comm.eng.osaka-u.ac.jp

Received 13 July 2021; Revised 14 September 2021; Accepted 11 October 2021; Published 29 November 2021

Academic Editor: Shifeng Sun

Low output locality is a property of functions, in which every output bit depends on a small number of input bits. In IoT devices with only a fragile CPU, it is important for many IoT devices to cooperate to execute a single function. In such IoT's collaborative work, a feature of low output locality is very useful. This is why it is desirable to reconstruct cryptographic primitives with low output locality. However, until now, commitment with a constant low output locality has been constructed by using strong randomness extractors from a nonconstant-output-locality collision-resistant hash function. In this paper, we construct a commitment scheme with output locality-3 from a constant-output-locality collision-resistant hash function for the first time. We prove the computational hiding property of our commitment by the decisional (M, δ)-bSVP assumption and prove the computational binding property by the (M, δ)-bSVP assumption, respectively. Furthermore, we prove that the (M, δ)-bSVP assumption can be reduced to the decisional (M, δ)-bSVP assumption. We also give a parameter suggestion for our commitment scheme with the 128 bit security.

1. Introduction

The computational complexity of cryptographic primitives is a fundamental problem in the construction of highly efficient and secure protocols [1, 2]. In ITCS 2017, Applebaum et al. achieved pioneering results for low-complexity cryptographic constructions of fundamental primitives [3]. Their technique provides a general framework for converting relatively high-complexity cryptographic functions to low-complexity ones, including one-way and pseudorandom functions of low output localities. Furthermore, Applebaum et al. proposed constructions for collision-resistant hash functions of a constant output locality from computationally hard problems of lattices and multivariate polynomials [4]. Interestingly, one of their collision-resistant hash functions with low output locality relies on the hardness assumption of the lattice problem called (M, δ)-bSVP assumption.

The output locality is a natural complexity measure of computational efficiency for Boolean functions. It is known that a Boolean function has output locality k if each output bit depends on a maximum of k input bits. It is obvious that low-output locality functions are implementable by low-depth circuits, implying high parallelizability. In extreme cases, if a function has a constant output locality, it can be decomposed into smaller functions computed using constant-depth circuits in parallel. In IoT devices with only a fragile CPU, it is difficult to execute a single rather large function. For this reason, it is important for many IoT devices to cooperate to execute a single function. In such IoT's collaborative work, the decomposition property into smaller functions is very useful. Low-depth cryptographic functions play crucial roles in certain protocols as well as IoT devices. For example, the bootstrapping method requires a low-depth decryption function as in lattice-based fully homomorphic public-key encryption [5].

There are several quantum-resistant cryptosystems, such as homogeneous cryptosystems and lattice cryptosystems. Output locality is a technology that encourages collaborative work on cryptography. In particular, the construction of cryptographic primitives that are secure against quantum cryptography and satisfy output locality is significant for the widespread use of IoT devices. This paper aims to construct cryptographic primitives that have output locality and are secure against quantum cryptography.

On the contrary, a commitment scheme is a fundamental protocol and a key building block of basic cryptographic tasks such as zero-knowledge identification [6]. The scheme is conducted between two parties (i.e., a sender and a receiver) through commitment and decommitment phases. In the commitment phase, the sender converts a message into a commitment string and sends it to the receiver. Then, in the decommitment phase, the sender sends the decommitment string where the message is embedded, which allows the receiver to verify if the commitment string was indeed generated from the message or not. A commitment scheme's security is formalized based on two properties: the hiding property and the binding property. The hiding property guarantees that no receiver can receive partial information of messages before the decommitment phase. Simultaneously, the binding property ensures that no sender can choose one of more than two candidate messages by switching the decommitment strings in the decommitment phase.

The related work is as follows. Note that neither standard commitment schemes such as Pedersen [7] nor Halevi-Micali [8] have low output localities. To achieve a commitment scheme with low output locality, two approaches have been investigated until now. One is proposed in [3], where a transformation from collision-resistant hash functions to commitment schemes that preserve low output locality by using strong randomness extractors in order to obtain the hiding property is provided. Their commitment schemes using this general transformation satisfy the output locality of four.

Another one is to avoid using such strong randomness extractors and to construct a commitment scheme directly from a hash function [9, 10], which are our preliminary works. Remark that, in [9], it only proves that the output locality is smaller than the input length, and in [10], it is only claimed that the hiding property is based on the decisional (M, δ)-bSVP assumption, whereas no concrete proof was given nor the relation between the decisional (M, δ)-bSVP assumption and (M, δ)-bSVP assumption was shown. In other words, no secure commitment with output locality-3 has been proposed so far without using strong randomness extractors.

Our contributions are as follows. In this paper, we propose a commitment scheme with an output locality of three for the first time. Our construction does not use strong randomness extractors. We construct a commitment scheme directly from a collision-resistant hash function in NC^0 without using a strong randomness extractor. We prove its computational hiding property and its computational binding property by using the decisional (M, δ)-bSVP assumption and (M, δ)-bSVP assumption, respectively. Furthermore, we prove that the (M, δ)-bSVP assumption can be reduced to the decisional (M, δ)-bSVP assumption.

To construct such a commitment scheme, we focus on two primitives. The first is a commitment scheme from the short integer solution (SIS) problem [11]. This scheme makes use of a lattice-based collision-resistant hash function of a "matrix-vector multiplication" form, i.e., $y = M \cdot x$ for a matrix $M \in \mathbb{Z}_q^{m \times n}$, and a vector $x \in \mathbb{Z}_2^n$. Our commitment also follows such a simple construction. As for the lattice-based collision-resistant hash function of low output locality, we use the next primitive of a function $f(x) = M \cdot \mathrm{ex}(x)$, where ex is an expanding function that dilutes the Hamming weight on the input x to achieve collision-resistant properties from the intractability of bSVP [3]. Then, a randomized encoding technique [4] is applied to the function $f(x)$ to achieve low output locality. Here, a randomized encoding of $f(x)$ is a randomized mapping $\widehat{f}(x, r)$ that generates an output distribution dependent only on $f(x)$.

Compared to previous works [10] in CANDAR 2020, this paper is the full version of the paper presented at CANDAR 2020. In our preliminary work [10], we have constructed a commitment scheme with output locality-3. However, it does not include any security consideration. In this article, we reconstruct a commitment scheme with output locality-3 based on the (M, δ)-bSVP assumption and decisional (M, δ)-bSVP assumption. We describe what we have achieved in this paper in the following:

(i) Prove that the (M, δ)-bSVP assumption can be reduced to the decisional (M, δ)-bSVP assumption

(ii) Prove that our commitment scheme satisfies the computational binding property based on the (M, δ)-bSVP assumption and satisfies the computational hiding property based on the decisional (M, δ)-bSVP assumption

(iii) Compare our commitment scheme with other previous studies

Roadmap: the remainder of this paper is organized as follows. Section 2 summarizes the commitment scheme, the hash function, and the output locality. Section 3 describes the building blocks of our construction. Then, we present our commitment scheme in Section 4. In Section 5, we suggest the parameter of our commitment scheme. Finally, we conclude our work in Section 6.

2. Preliminaries

First, we summarize the notations used in this paper.

(1) 1^k: security parameter

(2) a: message string

(3) r: random string

(4) com: commitment string

(5) dec: decommitment string

(6) $\varepsilon(k)$: negligible function in k

(7) ex: expand function

(8) pp: public parameters

(9) $S(1^k, \mathrm{pp})$: probabilistic polynomial-time party

(10) $R(\mathrm{com}, \mathrm{dec})$: probabilistic polynomial-time party which executes in the decommitment phase

(11) $R_{\mathrm{com}}(\mathrm{pp}, \mathrm{com})$: probabilistic polynomial-time party which executes in the commitment phase

(12) c, d: output locality in the ex function

(13) $\perp$: rejection symbol output by R for invalid inputs

(14) $\mathrm{Hw}(x)$: Hamming weight of x

(15) $\Delta(x)$: the ratio of "1"s in x

(16) H_{Mex}: the hash function we used in this paper

(17) $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$: our proposed commitment scheme

(18) $\mathbb{N}$: set of natural numbers

(19) $m < n \in \mathbb{N}$

(20) $\mathscr{M}(1^n)$: matrix sampler that generates a uniformly random $m \times n$ matrix.

(21) $H_2(p) = -p \log_2(p) - (1-p)\log_2(1-p)$ denotes the binary entropy function, where $p \in [0, 1]$

(22) ε: a negligible function throughout this paper

Next, we define the commitment scheme, which is as follows [12].

Definition 1 (commitment scheme). A commitment scheme, $\mathrm{Comm}(S, R)$, is a two-phase protocol between two probabilistic polynomial-time parties S and R, which are called the sender and receiver, respectively.

During the first phase (commitment phase), S commits string a to a pair of keys $(\mathrm{com}, \mathrm{dec})$ by executing $(\mathrm{com}, \mathrm{dec}) \leftarrow S(1^k, \mathrm{pp})$. Then, S sends com (commitment string) to R.

During the second phase (decommitment phase), S sends the keys dec (decommitment string) with a to R. Then, R verifies whether the decommitment string is valid by executing $R(\mathrm{com}, \mathrm{dec})$. If invalid, $R(\mathrm{com}, \mathrm{dec})$ outputs a special string, $\perp$, meaning that R rejects the decommitment of S. Otherwise, $R(\mathrm{com}, \mathrm{dec})$ can efficiently compute the string a revealed by S and verifies whether a was indeed chosen by S during the first phase.

In the following discussion, we provide the security notions of the commitment scheme $\mathrm{Comm}(S, R)$.

Definition 2 (computational binding property; see [8]). We state that $\mathrm{Comm}(S, R)$ is computationally binding if it is computationally infeasible to generate a commitment string com and two decommitment strings, $\mathrm{dec}, \mathrm{dec}'$ $(\mathrm{dec} \neq \mathrm{dec}')$, such that R will compute a message a from $(\mathrm{com}, \mathrm{dec})$ and a different message a' from $(\mathrm{com}, \mathrm{dec})$. In detail, for every probabilistic polynomial-time adversary $S'(1^k, \mathrm{pp})$, the following occurs:

$$\Pr\left[\begin{array}{cc} & R(\mathrm{com}, \mathrm{dec}) \neq \perp \\ (\mathrm{com}, \mathrm{dec}, \mathrm{dec}') \leftarrow S'\left(1^k, \mathrm{pp}\right): & R(\mathrm{com}, \mathrm{dec}') \neq \perp \\ & R(\mathrm{com}, \mathrm{dec}) \\ & \neq R(\mathrm{com}, \mathrm{dec}') \end{array}\right] < \varepsilon(k), \quad (1)$$

where $\varepsilon(k)$ is a negligible function of k. We then say that the commitment scheme $\mathrm{Comm}(S, R)$ is computationally binding.

Definition 3 (computational hiding property). A commitment scheme $\mathrm{Comm}(S, R)$ is computationally hiding if for every probabilistic polynomial-time party R_{com}, it satisfies

$$\left|\Pr_{y_1}[R_{\mathrm{com}}(\mathrm{pp}, y_1) = 1] - \Pr_{y_2}[R_{\mathrm{com}}(\mathrm{pp}, y_2) = 1]\right| < \varepsilon(k), \quad (2)$$

where pp is a public parameter generated randomly according to the commitment scheme and y_i is a commitment string generated from pp and x_i by S for random x_i sampled from an unknown distribution to R_{com} $(i = 1, 2)$.

The computational security of a commitment scheme in this study uses the following assumption.

Definition 4 ($(M, \boldsymbol{\delta})$-bSVP assumption; see [3]). For a weight parameter, $\delta(n), \delta: \mathbb{N} \longrightarrow (0, 1/2)$, and an efficient sampler $\mathscr{M}(1^n)$ that samples $m \times n$ binary matrices, the (M, δ)-bSVP assumption asserts that, for every efficient algorithm Adv, the probability is given by

$$\Pr_{M \xleftarrow{R} \mathscr{M}(1^n)}[\mathrm{Adv}(M) = x\ s.t. \mathrm{Mx} = 0 \text{ and } \Delta(x) \leq \delta] < \varepsilon(n). \quad (3)$$

We introduce a feature of the output locality. We start from the definition of a hash function. A hash function converts input bits of arbitrary length into compressed output bits of shorter lengths. We define the collision resistance of a hash function in Definition 5.

Definition 5 (collision resistance). We have an arbitrary probabilistic polynomial algorithm, Adv, given a description of the hash function and length parameter as inputs. If the probability of Adv that outputs $x, x' \in \{0, 1\}^k$ satisfying $x \neq x'$ and $f(x) = f(x')$ is negligible, the function is a collision-resistant hash function.

$$\Pr\left[\mathrm{Adv}\left(f, 1^k\right) \longrightarrow (x, x') s.t. x \neq x', f(x) = f(x')\right] < \varepsilon(k). \quad (4)$$

Next, we define the output locality.

Definition 6 (output locality). We say that the function h has output locality d if each of the output bits depends on at most d input bits.

Finally, we define perfect randomized encoding (PRE). PRE is a technique that can make the output locality a constant.

Definition 7 (perfect randomized encoding; see [3]). Let $f: \{0, 1\}^n \longrightarrow \{0, 1\}^l$ be a function. We say that a function $\hat{f}: \{0, 1\}^n \times \{0, 1\}^m \longrightarrow \{0, 1\}^s$ is a PRE of f if there exist an efficient decoding algorithm C and a randomized simulator S that satisfy the following:

(i) Perfect correctness: for every input $x \in \{0, 1\}^n$ and $r \in \{0, 1\}^m$, $C(\widehat{f}(x; r)) = f(x)$ holds

(ii) Perfect privacy: for every $x \in \{0,1\}^n$, the distribution $\widehat{f}(x;r)$ induced by a uniform choice of $r \overset{R}{\longleftarrow} \{0,1\}^m$ is identical to the distribution of $S(f(x))$

(iii) Balanced simulation: the distribution $S(y)$ induced by choosing $y \overset{R}{\longleftarrow} \{0,1\}^l$ is identical to the uniform distribution over $\{0,1\}^s$

(iv) Length preserving: the difference between the output length and the total input length of the encoding $s - (n+m)$ is equal to the difference $l - n$ between the output length and the input length of f

3. Building Blocks

In this section, we first define an expanding function ex [3] in Section 3.1. The expanding function is created for the function to apply the (M,δ)-bSVP assumption. We then show an example of PRE and how to make the output locality constant by using PRE in Section 3.2. We also show how to gain $f(x)$ from encoded function $\widehat{f}(x)$, which is called perfect correctness in PRE.

3.1. Expand Function ex. We give one expanding function ex used in Theorem 4, where ex is a function of $\{0,1\}^k \longrightarrow \{0,1\}^n$ that dilutes the relative Hamming weight of the input bits. In order to satisfy the (M,δ)-bSVP assumption, the relative Hamming weight β of the outputs of $\mathrm{ex}(x)$ has to satisfy $\beta \le \delta/2\,(\delta \in (0,1/2))$.

Next, we will explain how the function ex expands the input bits. First, we divide k bit blocks to k/d bit blocks, in which each bit block has d bits, as shown in Figure 1. We execute a function ex0 to each of the d bit blocks, where ex0 expands d bit blocks to c bit blocks, shown in Algorithm 1. Then, every block of the output of ex0 is concatenated as an output of ex $(c \cdot (k/d) = n)$. The whole algorithm of ex is given in Algorithm 2. The feature of ex is given in Lemma 1.

Lemma 1 (expand function with low output locality; see [3]). *For $\delta \in (0,1/2)$, let $\beta \le \delta/2$ be the relative Hamming weight of ex. Set $n/k \ge \lceil 1/H_2(\beta) \rceil$ and $c \ge \lceil 1/H_2(\beta) \rceil d$ for the natural numbers n, k. Then, there exists an efficiently computable function ex: $\{0,1\}^k \longrightarrow \{0,1\}^n$ such that (1) ex is injective, (2) $\Delta(ex(x)) \le \beta$ for every x, and (3) ex has output locality d.*

In this study, the hash function H_{Mex} uses an expanding function defined in Lemma 1.

3.2. Construction of PRE. We give one construction of PRE for a given function $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ in 1.

Construction 1 (see [1]). Let f be a function $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. Then, we separate $f(x)$ to v functions $T_1, \ldots, T_v\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ as follows:

$$f(x) = T_1(x) + \cdots + T_v(x), \tag{5}$$

where $T_j(x)$ can be written by monomial $(j = 1, \ldots, v)$. For $r_1, \ldots, r_v, r'_1, \ldots, r'_{v-1} \in \mathbb{F}_2$, we define a function $\widehat{f}\colon \mathbb{F}_2^n \times \mathbb{F}_2^{2v-1} \longrightarrow \mathbb{F}_2^{2v}$ by

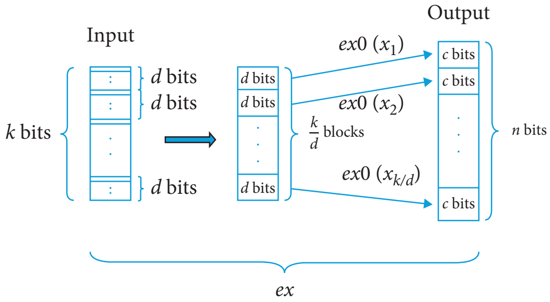

Figure 1: ex function.

$$\begin{aligned}&\widehat{f}(x,(r_1,\ldots,r_v,r'_1,\ldots,r'_{v-1}))\\&\quad=(T_1(x)-r_1,T_2(x)-r_2,\ldots,T_v(x)-r_v,r_1\\&\qquad-r'_1,r'_1+r_2-r'_{v-2}+r_{v-1}-r'_{v-1}+r_v).\end{aligned}\tag{6}$$

1 satisfies PRE in Definition 7. Let $f(x) = x_1x_2 + x_2x_3 + x_4$ where $v = 3$ and $n = 4$. Then, f can be encoded as the following equation:

$$\begin{aligned}&\widehat{f}(x,(r_1,r_2,r_3,r'_1,r'_2))\\&\quad=(x_1x_2-r_1,x_2x_3-r_2,x_4-r_3r_1-r',r'_1+r_2-r'_2,r'_2+r_3).\end{aligned}\tag{7}$$

Equation (7) is an example of 1. Denote by $C(z)$ adding all bits in z over $\mathbb{F}_2$. Then, we can gain $f(x)$ from $\widehat{f}(x)$ by using C as follows:

$$\begin{aligned}C(\widehat{f}(x))&=x_1x_2-r_1+x_2x_3-r_2+x_4-r_3++r_1\\&\quad-r'_1+r'_1+r_2-r'_2+r'_2+r_3\\&=x_1x_2+x_2x_3+x_4.\end{aligned}\tag{8}$$

It satisfies "perfect correctness" since $C(\widehat{f}(x)) = f(x)$. From the example of equation (7), the output locality of function $f(x)$ can be reduced to a constant by using PRE. A quantitative evaluation of the output locality is given in Lemma 2.

Lemma 2 (see [1]). *Let $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ be a function. Then, let $\widehat{f}$ be given as in 1. In particular, if f is a degree-d polynomial written as a sum of monomials, then $\widehat{f}$ is a PRE of f with degree d and output locality* $\max\{d+1,3\}$ *1.*

4. Proposed Commitment Scheme

In this section, we propose a commitment scheme $\mathrm{Comm}_{\mathrm{Mex}}(S,R)$ which is constructed by using ex and $\widehat{H}_{\mathrm{Mex}}$. The hash function $\widehat{H}_{\mathrm{Mex}}$ is PRE of H_{Mex}. We define the decisional (M,δ)-bSVP assumption and show that the (M,δ)-bSVP assumption can be reduced to the decisional (M,δ)-bSVP assumption. Furthermore, we show that our proposed commitment scheme satisfies the binding property and hiding property.

4.1. Difference between $\mathrm{Comm}_{Mex}(S,R)$ and the Commitment in [3]. In [3], Applebaum et al. showed how to construct a

```
    Input: $x \in \{0,1\}^d$
    Output: $\mathrm{ex0}(x) \in \{0,1\}^c$
(1) Identify $x \in \{0,1\}^d$ as a binary representation of natural numbers in $\{0,\ldots,2^d-1\}$
(2) Set $y \in \{0,1\}^c$ to the $(x+1)$-th string of a relative Hamming weight of maximum value $\beta$ in the lexicographic order
(3) Return $y \in \{0,1\}^c$
```

Algorithm 1: ex0 function.

```
    Input: $x \in \{0,1\}^k$
    Output: $\mathrm{ex}(x) \in \{0,1\}^n$
(1) Partition $k$-bit inputs into $k/d$ input blocks of $d$ bits each
(2) Apply ex0 to each input block, and generate $k/d$ output blocks of $c$ bits
(3) Return $\mathrm{ex0}(x_1)\mathrm{ex0}(x_2)\ldots\mathrm{ex0}(x_{k/d}) = \mathrm{ex}(x)$
```

Algorithm 2: ex function.

statistically hiding commitment scheme with output locality-4 from their collision-resistant hash function under the (M,δ)-bSVP assumption. Their commitment scheme executes a hash function based on a randomness extractor and an ordinary hash function with output locality-4. As a result, two hash functions are required. Furthermore, the randomness extractor is the universal hash function family, so it requires additional random bits to choose a function from the function family. Here, additional bits correspond to the input of the hash function.

On the contrary, our commitment scheme has to only execute an ordinary hash function once. Compared with their commitment scheme, our scheme is more efficient. Furthermore, our commitment scheme achieves output locality-3 by introducing the new notion of decisional (M,δ)-bSVP assumption.

4.2. Decisional (M,δ)-bSVP Assumption.

We introduce a new notion of decisional (M,δ)-bSVP assumption, which is a decisional version of the (M,δ)-bSVP assumption defined in Definition 4.

Definition 8 (decisional (M,δ)-bSVP assumption). For a weight parameter $\delta(n)$: $\mathbb{N} \longrightarrow (0,1/2)$, a uniform distribution $U \in \mathbb{Z}_2^m$, and an efficient sampler $\mathcal{M}(1^n)$ that samples $m \times n$ binary matrices, the decisional (M,δ)-bSVP assumption asserts that, for any polynomial algorithm Adv and for every $x \in \{0,1\}^n$ where $\delta \le \Delta(x) \le 1-\delta$,

$$\left| \Pr_{M \overset{R}{\leftarrow} \mathcal{M}(1^n), y_1 \leftarrow M\cdot x} \left[\mathrm{Adv}(M, y_1) = 1\right] - \Pr_{M \overset{R}{\leftarrow} U, y_2 \leftarrow U} \left[A\ dv(M, y_2) = 1\right] \right| < \varepsilon(n). \quad (9)$$

We show that the (M,δ)-bSVP assumption can be reduced to the decisional (M,δ)-bSVP assumption by referring to the methodology presented in Lemma 4.2 of [13], where Decision LWE is reduced to Search LWE.

Theorem 1. *Let y: $\{0,1\}^n \longrightarrow \{0,1\}^m$ be a function, and define (M,δ)-bSVP distribution on m-bit strings obtained by choosing $x \in \{0,1\}^n$ and outputting $y = M \cdot x$. Assume that we have an access to a procedure D which distinguishes the input y sampled from the distribution of (M,δ)-bSVP or sampled from a uniform distribution U with nonnegligible probability. Then, there exists a polynomial-time algorithm D' such that given samples from (M,δ)-bSVP distribution, D' can output x with nonnegligible probability.*

Proof. Let D be a distinguisher which distinguishes an element sampled from the (M,δ)-bSVP distribution or sampled from a uniform distribution U. Then, we construct D' which finds $x \in \mathbb{Z}_2^n$ of Mx. We first show how D' finds $x_1 \in \mathbb{Z}_2$ which denotes the first coordinate of x. The remaining coordinates can be recovered by the same way.

Given an input of D', $A = (M, y)$, where y is selected from an (M,δ)-bSVP distribution. The input of D can be defined as follows. Let x be denoted as $x = [x_1,\ldots,x_n]$ and M be denoted by the following equation:

$$M = \begin{pmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1n} \\ \vdots & \ddots & & & \vdots \\ c_{i1} & & c_{ij} & & c_{in} \\ \vdots & & & \ddots & \vdots \\ c_{m1} & \cdots & c_{mj} & \cdots & c_{mn} \end{pmatrix}. \quad (10)$$

Then, $y = Mx \in \mathbb{F}_2^m$ can be written as

$$y = \begin{pmatrix} c_{11}\cdot x_1 \oplus c_{12}\cdot x_2 \oplus \cdots \oplus c_{1n}\cdot x_n \\ \vdots \\ c_{m1}\cdot x_1 \oplus c_{m2}\cdot x_2 \oplus \cdots \oplus c_{mn}\cdot x_n \end{pmatrix}. \quad (11)$$

For randomly chosen $k \in \mathbb{Z}_2$ and $l_{i1} \in \mathbb{Z}_2$ $(i = 1, \ldots, m)$, compute a pair

$$A' = \left(M \oplus \begin{pmatrix} l_{11} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ l_{m1} & 0 & \cdots & 0 \end{pmatrix}, y \oplus \begin{pmatrix} l_{11}\cdot k \\ \vdots \\ l_{m1}\cdot k \end{pmatrix} \right). \quad (12)$$

Denote the value obtained in equation (12) as $A' = (M', y')$. Now, D' sends $A' = (M', y')$ to D. If $k = x_1$, then y' can be written as the following equation:

$$y' = \begin{pmatrix} (c_{11} \oplus l_{11})\cdot x_1 \oplus \cdots \oplus c_{1n}\cdot x_n \\ \vdots \\ (c_{m1} \oplus l_{m1})\cdot x_1 \oplus \cdots \oplus c_{mn}\cdot x_n \end{pmatrix}. \quad (13)$$

Since equation (13) can be expressed in the form $y' = M'x$, D can distinguish that equation (13) is contained in the (M, δ)-bSVP distribution. Then, D can distinguish that A' is in the (M, δ)-bSVP distribution. In contrast, if $k \neq x_1$, then y' will be expressed as

$$y' = Mx \oplus \begin{pmatrix} l_1 k \\ \vdots \\ l_m k \end{pmatrix}, \quad (14)$$

which is clearly not a sample from the (M, δ)-bSVP distribution. Then, D can distinguish that A' is in the uniform distribution.

Finally, D' outputs $k = x_1$ if D outputs (M, δ)-bSVP distribution. On the contrary, D' outputs $k = \overline{x}_1$ if D outputs uniform distribution.

All other remaining coordinates in x can be recovered in the same way. Therefore, D' can output x by using D with nonnegligible probability.

From the contraposition of Theorem 1, we can get Corollary 1. □

Corollary 1. *There is no polynomial algorithm that can break the decisional (M, δ)-bSVP assumption under the hardness of the (M, δ)-bSVP assumption.*

4.3. Proposed Commitment Scheme $\mathrm{Comm}_{Mex}(S, R)$. We analyze the hash function $\widehat{H}_{\mathrm{Mex}}$ in Section 4.3.1 and show our commitment scheme $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$ in Section 4.3.2.

4.3.1. A Hash Function $\widehat{H}_{Mex}$ for the Commitment Scheme. We first explain a hash function H_{Mex} [3], containing a matrix MM and an expand function ex, as shown in Algorithm 3.

Then, we show the hash function $\widehat{H}_{\mathrm{Mex}}$ which is PRE of H_{Mex}.

$$\widehat{H}_{\mathrm{Mex}}\colon \{0,1\}^k \times \{0,1\}^{nm} \longrightarrow \{0,1\}^{(1+n)m}. \quad (15)$$

We consider the matrix M as follows:

$$M = \begin{pmatrix} c_{11} & \cdots & c_{1j} & \cdots & c_{1n} \\ \vdots & \ddots & & & \vdots \\ c_{i1} & & c_{ij} & & c_{in} \\ \vdots & & & \ddots & \vdots \\ c_{m1} & \cdots & c_{mj} & \cdots & c_{mn} \end{pmatrix} = \begin{pmatrix} M[1] \\ \vdots \\ M[i] \\ \vdots \\ M[m] \end{pmatrix}, \quad (16)$$

for $c_{i,j} \in \mathbb{Z}_2$ and $M[i] \in \{0,1\}^n$ $(i = \{1, \ldots, m\},\ j = \{1, \ldots, n\})$. Also, we define the random number $t \in \{0,1\}^{nm}$ as $t = [T[1], \ldots, T[m]]$ where $T[i]$ is taken over uniform $T[i] \in \{0,1\}^n$ in any $i \in \{1, \ldots, m\}$. Furthermore, define $\mathrm{ex}(x)$ as $\mathrm{ex}(x) = [\mathrm{ex}(x)[1], \ldots, \mathrm{ex}(x)[n]]$ where $\mathrm{ex}(x)[i]$ is taken over $\mathrm{ex}(x)[i]$ in any $i \in \{1, \ldots, n\}$. Note that we write the first coordinate of $T[1]$ as $t[1][1]$. An algorithm of $\widehat{H}_{\mathrm{Mex}}$ is shown in Algorithm 4. Note that a matrix $M \in \mathscr{M}(1^n)$ is treated as a part of the description of the algorithm.

The hash function $\widehat{H}_{\mathrm{Mex}}$ is PRE of H_{Mex} since the construction of $\widehat{H}_{\mathrm{Mex}}$ is as same as 1. Here, we only give a theorem about PRE of H_{Mex} and $\widehat{H}_{\mathrm{Mex}}$.

Theorem 2. *$\widehat{H}_{Mex}$ satisfies perfect correctness, perfect privacy, balanced simulation, and length preserving for H_{Mex}.*

We show the output locality of $\widehat{H}_{Mex}$ in Theorem 3.

Theorem 3. *$\widehat{H}_{Mex}$ has 3 output localities.*

Proof. Let us investigate the output locality of $\widehat{H}_{\mathrm{Mex}}$. From the structure of Algorithm 4, the maximum number of input bits on which the output bits depend is 3. Therefore, the output locality of $\widehat{H}_{\mathrm{Mex}}$ is 3.

Next, let us discuss the collision resistance of $\widehat{H}_{\mathrm{Mex}}$. If a function satisfies the collision resistance, then its PRE also satisfies the collision resistance [1]. Applebaum et al. proved the collision resistance of H_{Mex}. Therefore, the collision resistance of $\widehat{H}_{\mathrm{Mex}}$ follows from [1]. The collision resistance of $\widehat{H}_{\mathrm{Mex}}$ is described in Lemma 3. □

Lemma 3 (collision resistance of $\widehat{H}_{\mathrm{Mex}}$; see [3]). *Let the hash function $\widehat{H}_{Mex}$ be a perfectly randomized encoding of H_{Mex}. Then, $\widehat{H}_{Mex}$ has a collision resistance under the (M, δ)-bSVP assumption.*

4.3.2. Commitment Scheme $\mathrm{Comm}_{Mex}(S, R)$. We show the commitment scheme $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$ based on $\widehat{H}_{\mathrm{Mex}}$, which consists of initialization, a commitment phase, and a decommitment phase. In this construction, we use the same matrix M, but we can also refresh a matrix M in a certain period, and the computational binding property and computational hiding property also hold using refreshed matrix M. $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$:

Initialization:

```
Input: $x \in \{0,1\}^k$
Output: $\mathbf{M} \cdot \mathrm{ex}(x) \in \{0,1\}^m$
Partition $k$-bit inputs into $k/d$ input blocks of $d$ bits each
Apply ex0 to each input block, and generate $k/d$ output blocks of $c$ bits
Set $\mathrm{ex}(x)$ as $\mathrm{ex}(x) = \mathrm{ex0}(x_1)\,\mathrm{ex0}(x_2) \ldots \mathrm{ex0}(x_{k/d})$
Compute $\mathbf{M} \cdot \mathrm{ex}(x)$
Return $\mathbf{M} \cdot \mathrm{ex}(x)$
```

Algorithm 3: Hash function: $H_{\mathrm{Mex}}(x)$.

```
Input: $x \in \{0,1\}^k$, $t \in \{0,1\}^{nm}$
Output: $\widehat{y} \in \{0,1\}^{(1+n)m}$
Compute $\mathrm{ex}(x)$ from $x$
for $1 \le i \le m$ do
  for $1 \le j \le n+1$ do
    $v \leftarrow (n+1) * (i-1) + j$
    if $v = (n+1) * (i-1) + 1$ then
      $\widehat{y}[v] \leftarrow (M[i][1] \wedge ex(x)[1]) \oplus t[i][1]$
      else if $v = (n+1) * (i-1) + n + 1$ then
      $\widehat{y}[v] \leftarrow t[i][n]$
      else
      $\widehat{y}[v] \leftarrow (M[i][j] \wedge ex(x)[j]) \oplus t[i][j] \oplus t[i][j-1]$
      end if
    end for
  end for
  return $\widehat{y}$
```

Algorithm 4: Algorithm of $\widehat{H}_{\mathrm{Mex}}$.

Before the commitment phase, both S and R share the following information:

(i) Algorithm of ex: $\{0,1\}^k \longrightarrow \{0,1\}^n$
(ii) Matrix $M \in \mathscr{M}(1^n)$
(iii) 1^k: security parameter

Commitment phase by S:

(1) Choose a random number $r \in \{0,1\}^{k/2}$ as the key of the hash functions
(2) Choose a message string $a \in \{0,1\}^{k/2}$, and concatenate a and r as $x = a \| r$
(3) Choose a random number $t \in \{0,1\}^{nm}$ which is used for PRE
(4) Compute $\mathrm{ex}(x) \in \{0,1\}^n$
(5) Compute $\widehat{H}_{\mathrm{Mex}}(a, r, t) \in \{0,1\}^{(n+1)m}$
(6) Send $\mathrm{com}(a, r, t) = \widehat{H}_{\mathrm{Mex}}(a, r, t')$ as a commitment string com

Decommitment phase from S to R:

S executes the following:

(1) S sends $(a, r) \in \{0,1\}^{k/2} \times \{0,1\}^{k/2}$ and $t \in \{0,1\}^{nm}$ to R as a decommitment string dec

R executes the following:

(1) Compute $x = a \| r$ from dec.
(2) Compute $\mathrm{ex}(x)$.
(3) Compute the commitment string $\widehat{H}_{\mathrm{Mex}}(a, r, t)$ and check whether $\widehat{H}_{\mathrm{Mex}}(a, r, t) = \mathrm{com}$. If this is satisfied, R outputs a. Otherwise, R outputs $\perp$.

Next, we prove the computational binding property and computational hiding property of $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$. We first show the computational binding property.

Theorem 4. *$\mathrm{Comm}_{Mex}(S, R)$ satisfies the computational binding property under the (M, δ)-bSVP assumption.*

Proof. We assume that there exists a probabilistic polynomial-time (PPT) adversary Adv that breaks the computational binding property of the commitment scheme $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$. Then, Adv can derive the following equation, with nonnegligible function $\varepsilon'(k)$ from Definition 2.

$$\Pr\left[\mathrm{Adv}\left(1^k, M\right) \longrightarrow (\mathrm{com}, \mathrm{dec}, \mathrm{dec}') \wedge \mathrm{dec} \neq \mathrm{dec}'\right] > \varepsilon'(k) \tag{17}$$

From equation (17), $\mathrm{com} = \widehat{H}_{\mathrm{Mex}}(\mathrm{dec})$, and another PPT adversary Adv', we can lead the following equation:

$$\begin{aligned} \Pr\left[\mathrm{Adv}'\left(1^k, M\right) \longrightarrow (\mathrm{dec}, \mathrm{dec}') \wedge \widehat{H}_{\mathrm{Mex}}(\mathrm{dec}) \right. \\ \left. = \widehat{H}_{\mathrm{Mex}}(\mathrm{dec}') \wedge \mathrm{dec} \neq de\ c'\right] > \varepsilon'(k) \end{aligned} \tag{18}$$

This shows that if PPT Adv can break the computational binding property, it can also break the collision resistance of $\widehat{H}_{\mathrm{Mex}}$ from equation (18). However, we showed that $\widehat{H}_{\mathrm{Mex}}$ has a collision resistance under the (M, δ)-bSVP assumption in Lemma 3. Therefore, the commitment scheme $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$ satisfies the computational binding property under the (M, δ)-bSVP assumption based on the contradiction.

Next, we will prove the computational hiding property of $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$. □

Theorem 5. *$\mathrm{Comm}_{\mathrm{Mex}}(S, R)$ satisfies the computational hiding property under the decisional $(M, d/4c)$-bSVP assumption for a constant $c/d = n/k$.*

Proof. We assume that there exists a probabilistic polynomial-time adversary Adv that breaks the computational hiding property of $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$. For some distinct $a, a' \in \{0,1\}^{k/2}$, $r, r' \in \{0,1\}^{k/2}$, $t, t' \in \{0,1\}^{nm}$, and some nonnegligible function ε', we can derive the following equation:

$$\begin{aligned}&\left|\Pr\left[\mathrm{Adv}\left(M, \widehat{H}_{\mathrm{Mex}}(a\|r, t)\right) = 1\right]\right.\\&\quad\left.- \Pr\left[\mathrm{Adv}\left(M, \widehat{H}_{\mathrm{Mex}}(a'\|r', t')\right) = 1\right]\right| > \varepsilon'(k).\end{aligned} \tag{19}$$

Since the decoding procedure C of PRE is a polynomial-time algorithm, there exists a polynomial-time adversary Adv', which is a composition of the decoding procedure and Adv such that

$$\begin{aligned}&\left|\Pr\left[\mathrm{Adv}'(M, M \cdot \mathrm{ex}(a\|r)) = 1\right]\right.\\&\quad\left.- \Pr\left[\mathrm{Adv}'(M, M \cdot \mathrm{ex}(a'\|r')) = 1\right]\right| > \varepsilon'(k).\end{aligned} \tag{20}$$

By the hybrid argument, for some a,

$$\begin{aligned}&\left|\Pr\left[\mathrm{Adv}'(M, M \cdot \mathrm{ex}(a\|r)) = 1\right]\right.\\&\quad\left.- \Pr\left[\mathrm{Adv}'(M, U) = 1\right]\right| > \frac{\varepsilon'(k)}{2}.\end{aligned} \tag{21}$$

Since r is uniformly random over $\{0,1\}^{k/2}$, for every $a \in \{0,1\}^{k/2}$, we have $\Delta(a\|r) \in (1/8, 7/8)$, and hence, $\Delta(\mathrm{ex}(a\|r)) \in (d/(8c), 7\,d/(8c))$ for a constant $c/d = n/k$ with probability $1 - \exp(-\Omega(k))$ from the Chernoff bounds. This contradicts the decisional (M, δ)-bSVP assumption. □

4.4. Comparison. We compare our proposed commitment scheme with related works of [BDLOP18] and [KTX08] in Table 1. Both [BDLOP18] and [KTX08] are also based on lattice-based functions and consist of "matrix-vector multiplication" in the same way as us.

A commitment scheme [KTX08] can prove its hiding property statistically and its binding property by the SIS problem. However, it did not achieve constant output locality. A commitment scheme [BDLOP18] can prove its hiding property and binding property by DKS and SKS problems, respectively. Nevertheless, it also did not achieve constant output locality.

Table 1: Comparison of our proposed commitment scheme.

	Hiding	Binding	Output locality
[KTX08] [11]	Statistical	SIS	—
[BDLOP18] [14]	DKS	SKS	—
[AHIKV17] [3]	Statistical	bSVP	4
This paper	D-bSVP	bSVP	3

On the contrary, the commitment scheme [AHIKV17] has achieved output locality-4 with its statistically hiding property and its binding property based on the (M, δ)-bSVP assumption (bSVP). However, their commitment scheme was to execute hash functions twice with a randomness extractor. It was also difficult to construct a commitment scheme with output locality-3 by using a randomness extractor.

Our commitment scheme $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$ satisfies output locality-3 by proving its hiding property and binding property by the decisional (M, δ)-bSVP assumption (D-bSVP) and (M, δ)-bSVP assumption (bSVP), respectively. Our commitment scheme only executes the hash function $\widehat{H}_{\mathrm{Mex}}$ once and does not use a randomness extractor.

5. Parameter Suggestion for $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$

This section suggests some parameter settings of $\mathrm{Comm}_{\mathrm{Mex}}(S, R)$ under evaluation based on the short integer solution (SIS) problem in Definition 9.

Definition 9 ($\mathrm{SIS}_{q,m,b}$; see [11]). Given a prime q, a positive number b, and a matrix $MA \in \mathbb{Z}_q^{n\times m}$, the short integer solution ($\mathrm{SIS}_{q,m,b}$) problem is to find a nonzero vector $z \in \mathbb{Z}^m$ such that $Az \equiv 0 (\mathrm{mod} q)$ and $\|z\| \leq b$.

Let M be a matrix in $\mathbb{F}_2^{m\times n}$. Under the condition of $\Delta(x) \leq \delta$, the (M, δ)-bSVP can be reduced to a $\mathrm{SIS}_{q,m,b}$ problem in the lattice spanned by vectors in $\mathrm{Ker}(M)$, where $q = 2$ and $b = \sqrt{n \cdot \delta}$, namely, to solve our scheme is reduced to find a short vector $v (\|v\| \leq \|x\|)$ in a lattice $L = \{v \in \mathbb{Z}^n \colon Mv = 0 (\mathrm{mod} 2)\}$. Denote the norm of the shortest nonzero vector b_1 in ML and the second shortest vector independent with b_1 by λ_1 and λ_2, respectively. We estimate parameters as follows:

(1) Estimation of δ:

  (a) $\lambda_1(L) = \|x\| = \sqrt{n \cdot \delta}$.

  (b) $\lambda_2(L) \approx \sqrt{n/2\pi e} \cdot 2^{m/n}$ by Gaussian heuristic, where the volume of lattice ML is $\mathrm{vol}(L) = 2^m$ and e is the mathematical constant.

  (c) Denote by $\alpha = m/n$ and $\delta < \alpha/2$ because of the algebraic attack due to [3]. α shows the ratio between input length and output length.

  Therefore, we can get a bound of $\delta \leq 0.07$ and $0.14 \leq \alpha$ by $\lambda_1/\lambda_2 < 1.0$ according to the definition of λ_1 and λ_2 above.

(2) Evaluate the asymptotic complexity to solve a SVP by using Alkim et al.'s estimate proposed in [15], and it had been experimentally verified in [16]. We heuristically set $n = m/\alpha$, $\alpha = 5 \cdot \delta$, and $\delta \leq 0.07$. Then, we

Table 2: Parameter suggestions for m, n, and δ being used in our scheme $\mathrm{Comm}(S, R_{\mathrm{com}})$.

Security level	m	n	δ	β_{BKZ}
AES-128	128	426	0.06	376
AES-192	128	731	0.035	601
AES-256	128	1066	0.024	837

input the parameters of $(m, n, \delta, q = 2)$; Alkim et al.'s estimate can evaluate the minimal β_{BKZ} which means the target block size used in the lattice reduction algorithm BKZ [17].

Please refer to [18] for a lucid explanation of Alkim et al.'s estimate. We consider the scenario that one hashes 128 bit information, namely, we fix $m = 128$ in the estimate.

Table 2 shows parameter suggestions of our scheme $\mathrm{Comm}(S, R_{\mathrm{com}})$ with respect to security levels of NIST AES-128, AES-192, and AES-256, where β_{BKZ} is the required block size when using the BKZ algorithm to solve (M, δ)-bSVP. The security levels of "AES-128," "AES-192," and "AES-256" refer to three categories in the NIST PQC standardization project [19] in that the brute force attack on AES key search requires at least 2^{143}, 2^{207}, and 2^{272} classical computing gates, respectively.

6. Concluding Remarks

In this paper, we achieved the following:

(i) We proposed a new output locality-3 commitment scheme

(ii) We proved that the (M, δ)-bSVP assumption is reduced to the decisional (M, δ)-bSVP assumption

(iii) We proved that its computational binding property and computational hiding property are reduced to the (M, δ)-bSVP assumption and decisional (M, δ)-bSVP assumption, respectively

(iv) We evaluated a secure parameter set against the short integer solution (SIS) problem

Generally, it is easy to build protocols based on the decisional (M, δ)-bSVP assumption compared with the (M, δ)-bSVP assumption. Therefore, our proof would shed light on the new construction of protocols whose security is based on the decisional (M, δ)-bSVP assumption. Also, our method can be used with IoT devices with small CPUs since our method satisfies constant output locality and can be achieved in smaller CPUs. However, it is expected to achieve an output locality-3 commitment scheme with statistical hiding, which is considered an open problem in this work.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was partially supported by enPiT (Education Network for Practical Information Technologies) at MEXT, JSPS KAKENHI (Grant no. JP21H03443) and Ovation Platform for Society 5.0 at MEXT. This work was also supported by JSPS KAKENHI (Grant no. JP21K11751), Japan, JSPS Grant-in-Aid for Scientific Research (A) (nos. 16H01705 and 21H04879), (B) (no. 17H01695), and (C) (no. 21K11887), JSPS Grant-in-Aid for Young Scientists (B) (no. 17K12640), and MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) (Grant no. JPMXS0120319794).

References

[1] B. Applebaum, Y. Ishai, and E. Kushilevitz, "Cryptography in NC0," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 845–888, 2006.

[2] M. Naor and O. Reingold, "Synthesizers and their application to the parallel construction of pseudo-random functions," *Journal of Computer and System Sciences*, vol. 58, no. 2, pp. 336–375, 1999.

[3] B. Applebaum, N. Haramaty, Y. Ishai, E. Kushilevitz, and V. Vaikuntanathan, "Low-complexity cryptographic hash functions," in *Proceedings of the 8th Innovations in Theoretical Computer Science Conference, ITCS*, Berkeley, CA, USA, January 2017.

[4] B. Applebaum, "Garbled circuits as randomized encodings of functions, a primer," *Electronic Colloquium on Computational Complexity*, vol. 24, 2017.

[5] J. Groth, "Homomorphic trapdoor commitments to group elements," *Cryptology ePrint Archive*, vol. 7, 2009.

[6] I. Damg rard, "Commitment schemes and zero-knowledge protocols," in *Lectures On Data Security, Modern Cryptology In Theory And Practice, Volume 1561 of LNCS*, I. Damg Rard, Ed., Springer, Berlin, Germany, 1998.

[7] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proceedings of the CRYPTO '91, 11th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 1991.

[8] S. Halevi and S. Micali, "Practical and provably-secure commitment schemes from collision-free hashing," in *Proceedings of the Advances in Cryptology-CRYPTO '96, 16th Annual International Cryptology Conference*, pp. 201–215, Santa Barbara, California, USA, August 1996.

[9] H. Miyaji, A. Kawachi, and A. Miyaji, "String commitment scheme with low output locality," in *Proceedings of the 2019 14th Asia Joint Conference on Information Security*, pp. 32–39, Kobe, Japan, August. 2019.

[10] H. Miyaji, A. Miyaji, and Y. Wang, "Homomorphic commitment scheme with low output locality," in *Proceedings of the 2020 the Eighth International Symposium on Computing and Networking, CANDAR*, November 2020.

[11] A. Kawachi, K. Tanaka, and K. Xagawa, "Concurrently secure identification schemes based on the worst-case hardness of lattice problems," in *Proceedings of the Advances in Cryptology-ASIACRYPT 2008*, pp. 372–389, Melbourne, Australia, November 2008.

[12] G. Di Crescenzo, J. Katz, R. Ostrovsky, and A. Smith, "Efficient and non-interactive non-malleable commitment," in *Proceedings of the EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques*, pp. 40–59, Innsbruck Austria, May 2001.

[13] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, p. 34, 2009.

[14] C. Baum, I. Damgård, V. Lyubashevsky, S. Oechsner, and C. Peikert, "More efficient commitments from structured lattice assumptions," in *Proceedings of the Security and Cryptography for Networks-11th International Conference, SCN 2018*, D. Catalano and R. D. Prisco, Eds., pp. 368–385, Amalfi, Italy, September 2018.

[15] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange-a new hope," *USENIX Security Symposium*, pp. 327–343, 2016, Report number: 2015/1092.

[16] M. R. Albrecht, F. Göpfert, F. Virdia, and T. Wunderer, "Revisiting the expected cost of solving usvp and applications to LWE," in *Proceedings of the Advances in Cryptology-ASIACRYPT 2017*, pp. 297–322, Hong Kong, China, December 2017.

[17] Y. Aono, Y. Wang, T. Hayashi, and T. Takagi, "Improved progressive BKZ algorithms and their precise cost estimation by sharp simulator," in *Proceedings of the EUROCRYPT 2016-35th Annual International*, pp. 789–819, Vienna, Austria, May 2016.

[18] W. Wang, Y. Wang, A. Takayasu, and T. Takagi, "Estimated cost for solving generalized learning with errors problem via embedding techniques," in *Proceedings of the Advances in Information and Computer Security 2018*, pp. 87–103, Sendai, Japan, September 2018.

[19] Us Department of Commerce and National Institute of Standards and Technology, *Post-Quantum Cryptography*, https://csrc.nist.gov/projects/post-quantum-cryptography/, 2020.